INFORMATION AND COMPUTATION 77, 162–178 (1988)

How Robust Is the n-Cube?

BERND BECKER AND HANS-ULRICH SIMON

Fachbereich 10, Informatik, Universität des Saarlandes, D-6600 Saarbrücken, West Germany

The n-cube network is called *faulty* if it contains any faulty processor or any faulty link. For any number k we want to compute the minimum number $f(n, k)$ of faults which is necessary for an adversary to make every $(n-k)$-dimensional subcube faulty. Reversely formulated: The existence of an $(n-k)$-dimensional nonfaulty subcube can be guaranteed, if there are less than $f(n, k)$ faults in the n-cube. In this paper several lower and upper bounds for $f(n, k)$ are derived such that the resulting gaps are "small." For instance if $k \geqslant 2$ is constant, then $f(n, k) = \theta(\log n)$. Especially for $k=2$ and large n: $f(n, 2) \in [\lceil \alpha_n \rceil : \lceil \alpha_n \rceil + 2]$, where $\alpha_n = \log n + \frac{1}{2} \log \log n + \frac{1}{2}$. Or if $k = \omega(\log \log n)$ then $2^k < f(n, k) < 2^{(1+\varepsilon)k}$, with ε chosen arbitrarily small. The aforementioned upper bounds are obtained by analysing the behaviour of an adversary who makes "worst-case" distributions of a given number of faulty processors. For $k=2$ the "worst-case" distribution is obtained constructively. In the general case the constructive methods presented in this paper lead to a (rather "bad") upper bound which can be significantly improved by probabilistic arguments. The bounds mentioned above change if the notions are relativized with respect to some given parallel fault-checking procedure P. In this case only subcubes which are possible outputs of P must be made faulty by the adversary. The notion of *directed chromatic index* is defined in order to analyse the case $k=2$. Relations between the directed chromatic index and the chromatic number are derived, which are of interest in their own right. © 1988 Academic Press, Inc.

1. INTRODUCTION

The n-cube is one of the universal topologies of point to point networks, for which it is possible to efficiently implement a rich class of parallel algorithms (see, e.g., Pease, 1977). This class contains fundamental algorithms, such as, algorithms for sorting, routing, computing the Fourier–Transform, and for related problems.

In general, and for large n in particular, one has to cope with the problem of faulty processors and faulty links inside the network. A network is called *robust* if its performance does not decrease "too much" in case of topology changes. Efficient cooperation between the nonfaulty processors should be maintained. One measure for robustness is the connectivity of a network–graph. High degree of connectivity prevents the nonfaulty processors from being disconnected. Moreover, highly connected networks,

0890-5401/88 $3.00

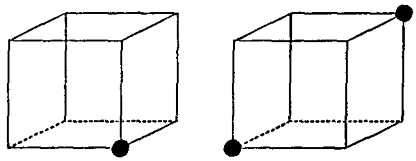

FIGURE 1

such as the n-cube, have the property that the diameter of the *surviving network*, i.e., the subnetwork induced by the nonfaulty processors and links, can be reasonably bounded, provided the number of faults does not exceed the dimension n (Chung and Garey, 1983). But even in this case the universality of a universal network would be lost, if, as a consequence of the topology changes, the fundamental algorithms had to be reorganized in a non-uniform and inefficient way.

Fortunately most of the basic algorithms for universal networks, such as n-cube, CCC, Butterfly, or Shuffle-Exchange, have the property that they can be formulated with the dimension of the network as a parameter of the algorithm. Thus they can be performed on any nonfaulty d-dimensional substructure with a slow down factor of 2^{n-d} (see the remarks about "limited parallelism" in (Preparata and Vuillemin, 1981) and the simulations between various universal networks in (Siegel, 1979)).

This gives rise of the question: What is the maximum number of dimensions that would be lost if the network contained r faulty processors or links? In this paper we will answer this question concerning the n-cube. It goes without saying that one faulty processor or link destroys one dimension. Two processors destroy two dimensions iff their addresses are related by bitwise negation. Similarly it can be shown that three links are necessary to destroy two dimensions. Figures 1 and 2 illustrate these observations. Fortunately, for general n, it is much harder to destroy 3 dimensions, even if an "intelligent" adversary is allowed to distribute the faulty processors

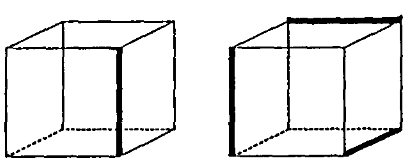

FIGURE 2

and faulty links in a "worst-case fashion." From now on we assume that $k \geqslant 2$.

By $f(n, k)$ we denote the minimum number of faults, necessary for an adversary to destroy $k+1$ dimensions (i.e., to make each $(n-k)$-dimensional subcube faulty). In this paper several lower and upper bounds for $f(n, k)$ are derived such that the resulting gaps are "small." First, we confine ourselves to assuming that only processors are faulty (= *faulty processor case*). Later we show how to derive analogous results for faulty links (= *faulty link case*), and for the case where both links and processors may be faulty. For intance, if $k \geqslant 2$ is constant, then we have in all cases $f(n, k) = \theta(\log n)$. Especially for $k=2$ and large n we show for the faulty processor case: $f(n, 2) \in [\lceil \alpha_n \rceil : \lceil \alpha_n \rceil + 2]$, where $\alpha_n = \log n + \frac{1}{2} \log \log n + \frac{1}{2}$. Or if k grows asymptotically faster than $\log \log n$, i.e., $k = \omega(\log \log n)$, then for almost all n $2^k < f(n, k) < 2^{(1+\varepsilon)k}$, which ε chosen arbitrarily small.

The above-mentioned upper bounds are obtained by analysing the behaviour of an adversary, who makes "worst-case" distributions of a given number of faulty processors. For $k=2$ the distribution is obtained constructively. In general $f(n, k)$ is bounded from above by using counting arguments. We also give constructive methods leading to a "worse" upper bound.

The above-mentioned bounds change if the notions are relativized with respect to some given parallel fault-checking procedure P. In this case only subcubes which are possible outputs of P must be made faulty by the adversary. For $k=2$ the notion of *directed chromatic index* is defined to analyse this situation. Relations between the directed chromatic index and the chromatic number are derived, which are of interest in their own right.

2. The Faulty Processor Case

We first consider the case where faults are restricted to faulty processors and then derive corresponding results for the remaining cases.

Reformulation of the Problem and Some Trivial Bounds

A *k-monomial* over the set $\{X_1, ..., X_n\}$ of *variables* is an expression $X_{i_1}^{\varepsilon_1} \cdots X_{i_k}^{\varepsilon_k}$, where the i_j are pairwise different indices from $[1:n]$ and the ε_j are 0 or 1, according to the identification $X^0 = \bar{X}$ and $X^1 = X$. $(\varepsilon_1, ..., \varepsilon_k)$ is called the *negation mask* of the monomial. To each k-monomial corresponds a unique $(n-k)$-dimensional subcube. Dimension i of this subcube is degenerated to ε iff the monomial contains X_i^{ε}. For instance, $\bar{X}_1 X_2$ specifies a unique edge in the 3-dimensional cube as illustrated in Fig. 3. A monomial is called *faulty* with respect to some given set

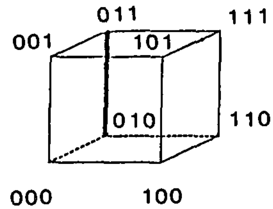

FIGURE 3

$F \subseteq \{0, 1\}^n$ of faulty processors, if the corresponding subcube contains any faulty processor from F. Reversely F is called k-faulty if it makes each k-monomial faulty.

To each set F of r faulty processors corresponds a $(n \times r)$-matrix $M_F \in \{0, 1\}^{n \times r}$ whose ith column vector gives the address of the ith faulty processor. If we fix an order in F the matrix M_F is uniquely determined. The row vectors may be interpreted as characteristic vectors for subsets of $[1:r]$. Thus a unique system $A_F = A = \{A_1, ..., A_n\}$ of such subsets is associated to F. A_F is called the system of *faulty sets*. The following lemma gives a useful reformulation of the problem with which we are dealing.

LEMMA 1. *F is k-faulty iff for all k-monomials over the set A_F*

$$A_{i_1}^{\varepsilon_1} \cap \cdots \cap A_{i_k}^{\varepsilon_k} \neq \emptyset,$$

where $B^0 = \bar{B}$ and $B^1 = B$ for each set $B \subseteq [1:r]$.

If F is k-faulty, the matrix M_F and the faulty set system A_F are called k-faulty, too. In (Kleitman and Spencer, 1973) the notion *k-faulty* is replaced by *k-independent* for systems A_F of sets and some properties of k-independent systems are shown. We apply a result of *op cit.* for 2-independent sets (Theorem 1) and obtain similar results for general k (Theorem 4). Figure 4 contains an example for a 2-faulty (10×6)-matrix.

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

FIGURE 4

In the following we will be dealing with the determination of $f(n, k)$, which can now be interpreted as the minimum r, such that a k-faulty $(n \times r)$-matrix exists. Before doing so, however, the following obvious inequalities should be mentioned.

LEMMA 2. $2^k \leqslant f(n, k) \leqslant (1/(n-k+1)) \cdot 2^n$.

Proof. The first inequality holds, because in particular all 2^k monomials using the first k variables must be made faulty. But these monomials specify pairwise disjoint subcubes. The second inequality is obtained by partitioning the set $\{0, 1\}^n$ of vertices in the n-cube into classes C_i, such that the sum of ones in each vertex of C_i is congruent to i module $n-k+1$. Then the smallest of these classes can be chosen as system of faulty processors. (Note, that for $k=n-1$ this strategy is optimal and results in $f(n, n-1) = 2^{n-1}$.) ∎

A Close Look at the $(k=2)$-Case

By $(2^r, \subset)$ we denote the poset of subsets of $[1:r]$. In the following result we use the theorem of Sperner (1928) and a modification given in (Kleitman and Spencer, 1973): The theorem of Sperner states that the size of a maximum antichain in 2^r is exactly $\binom{r}{\lfloor r/2 \rfloor}$. Thus the system of all sets in 2^r with $\lfloor r/2 \rfloor$ elements forms a maximum antichain. Throughout the paper R_n denotes the minimum r such that $\binom{r}{\lfloor r/2 \rfloor} \geqslant n$. The modification in (Kleitman and Spencer, 1973) is as follows: The size of an antichain A in 2^r, such that for all $A_i, A_j \in A$, $A_i \cap A_j \neq \varnothing$ and $A_i \cup A_j \neq [1:r]$, is less or equal $\binom{r-1}{\lfloor r/2 \rfloor - 1}$. By r_n we denote the minimum r such that $\binom{r-1}{\lfloor r/2 \rfloor - 1} \geqslant n$.

THEOREM 1. $f(n, 2) = r_n$.

Proof. For each system of faulty processors the monomials of the form $\bar{X}_i X_j$ are faulty iff the faulty sets form an antichain in 2^r. The monomials of the form $X_i X_j$, resp. $\bar{X}_i \bar{X}_j$, are faulty iff the intersection of any two faulty sets, resp. the intersection of the complements of any two faulty sets, is unequal to the empty set. Thus $f(n, 2) \geqslant r_n$ follows from (Kleitman and Spencer, 1973; Schönheim, 1971).

$f(n, 2) \leqslant r_n$ can be seen as follows: Take all sets in $2^{r_n - 1}$ with cardinality $\lfloor r_n/2 \rfloor - 1$ and augment each set with the element r_n. The resulting system has $\binom{r_n - 1}{\lfloor r_n/2 \rfloor - 1} \geqslant n$ elements and is 2-faulty. (The matrix M_F given in Fig. 4 is constructed according to this strategy.) ∎

The following corollary relates R_n and r_n and gives an explicit term for R_n (and thus for r_n).

COROLLARY 1. (i) *If r_n is odd, then* $r_n = 1 + R_n$.

(ii) *If* $r_n := 2s+2$ *is even, then*

$$r_n = \begin{cases} 1 + R_n & \text{if } n > \binom{2s}{s} \\ 2 + R_n & \text{if } n \leqslant \binom{2s}{s}. \end{cases}$$

(iii) *For large n,*

$$R_n \in \{\lfloor \alpha_n \rfloor, \lceil \alpha_n \rceil\}$$

with $\alpha_n = \log n + \frac{1}{2} \log \log n + \frac{1}{2}$.

Sketch of the Proof. (i) and (ii) can be easily shown by using the definition of R_n, r_n and the following property:

$$\forall p \in \mathbf{N} \colon n \in I_p \Leftrightarrow R_n = p,$$

$$\forall q \in \mathbf{N} \colon n \in J_q \Leftrightarrow r_n = q,$$

if we define $\forall s \in \mathbf{N}$:

$$I_{2s} := \left(\binom{2s-1}{s-1} : \binom{2s}{s} \right],$$

$$I_{2s+1} := \left(\binom{2s}{s} : \binom{2s+1}{s} \right],$$

$$J_{2s+1} := \left(\binom{2s-1}{s-1} : \binom{2s}{s-1} \right],$$

$$J_{2s+2} := \left(\binom{2s}{s-1} : \binom{2s+1}{s} \right].$$

(iii) can be shown by applying the Stirling formula and some technical calculations. ∎

The Directed Chromatic Index

The last theorem guarantees the existence of nonfaulty subcubes of dimension $n-2$, whenever we are sure that less than r_n of the processors are faulty. It is not clear, however, that a parallel algorithm will in fact check all $2n(n-1)$ 2-monomials. With a given parallel fault-checking procedure P this leads to the following considerations: For all $i, j \in [1:n]$ we draw a directed edge (i, j) iff procedure P checks whether subcube $\bar{X}_i X_j$ is faulty. If the resulting directed graph is denoted by $\mathbf{G}_P = (V_P, E_P)$, the number of faulty processors required by the adversary to make all 2-monomials of the above form faulty, can be expressed in a graph-theoretical way as shown in the following:

A directed colouring of a (directed) graph $\mathbf{G}$ is an edge-colouring according to the rule that 2 adjacent edges (i, j), (j, k) must have different colours. The minimum number of colours required is called *directed chromatic index* of $\mathbf{G}$ and denoted by $c(\mathbf{G})$. Then we have

LEMMA 3. *The directed chromaic $c(\mathbf{G}_P)$ is identical to the number of faulty processors necessary to make all those monomials faulty which are of the form $\bar{X}_i X_j$ and which are checked by the procedure P.*

Proof. Given a set of faulty processors, each edge (i, j) may be coloured by one of the faulty processors in the subcube $\bar{X}_i X_j$. Reversely, given a colouring for $\mathbf{G}_P$, to each colour class C of edges we associate the monomial $M(C)$ which contains $\bar{X}_i X_j$ iff $(i, j) \in C$. It follows from the definition of the chromatic index that no variable in $M(C)$ occurs in both negated and non-negated form. Now it is sufficient to put one faulty processor in each subcube, specified by some $M(C)$. ∎

Upper and lower bounds for the index $c(\mathbf{G}_P)$ are obtained as follows: Let $\mathbf{G}$ be a directed graph. Then G denotes the undirected graph which results from $\mathbf{G}$ by neglecting the orientation of the edges and replacing multiple edges by a single edge.

Directed versions of G are obtained by fixing an orientation for each edge. The *doubly-directed version* of G is obtained by giving both orientations to each edge. Figure 5 shows the doubly-oriented version of the triangle. The directed chromatic indices $c'(G)$, $c''(G)$ of an undirected graph G are defined as directed chromatic index of a simplest, directed version or of the doubly-directed version of G, respectively. For the triangle $c' = 2$ and $c'' = 3$. Figure 5 indicates a colouring with 3 colours.

The index $c(\mathbf{G}_P)$ is bounded below and above by $c'(G_P)$ and $c''(G_P)$, respectively. The following 2 results relate c' and c'' to the *chromatic number* $\gamma(G)$ of G, i.e., the minimum number of colours for some vertex-colouring of G as usually defined.

THEOREM 2. $c'(G) = \lceil \log \gamma(G) \rceil$.

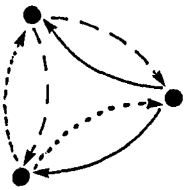

FIGURE 5

Proof. (i) We show: $\gamma(G) \leqslant 2^{c'(G)}$. Given an edge-colouring we may colour each vertex with the set of colours of its outgoing edges.

(ii) We show: $c'(G) \leqslant \lceil \log \gamma(G) \rceil$. The vertices are assumed to be coloured with the numbers $0, ..., \gamma - 1$. We direct edges (v, w) such that for the corresponding colours $g(v)$, $g(w)$: $g(w) < g(v)$. Thus there exists a bit position i such that the ith bits of $g(w)$ and $g(v)$ are 0 and 1, respectively. Then (v, w) may be coloured by the most significant of these bit positions. ▮

THEOREM 3. $c''(G) = R_{\gamma(G)}$.

Proof. (i) We show: $c'' \leqslant R_\gamma$. The vertex colours can be chosen as subsets of $[1 : R_\gamma]$ of size $\lceil R_\gamma/2 \rceil$. If A_x denotes the subset associated to vertex x, then any edge (v, w) can be coloured with $\max(A_v \backslash A_w)$.

(ii) We show: $c'' \geqslant R_\gamma$. We assume that the edges are coloured with numbers from $1, ..., c''$. To each vertex x we associate the set $A_x \subseteq [1 : c'']$ of colours of its outgoing edges. The resulting sets form a subposet A of $2^{c''}$. Let $C_1, ..., C_m$ be a minimum number of chains covering A. Since the subsets associated to neighbouring vertices of G must belong to different chains, we have $\gamma \leqslant m$. On the other hand there must be some antichain in A of size m by the theorem of Dilworth (1950). By Sperners theorem we get: $c'' \geqslant R_m \geqslant R_\gamma$. ▮

Note that Theorem 3 gives a second proof for $R_n \leqslant f(n, 2)$, taking advantage of the fact that n is the chromatic number of the n-clique. From Theorems 2 and 3 we also conclude

COROLLARY 2. *There is no polynomial time algorithm for the computation of the directed chromatic indices $c'(G)$, $c''(G)$ of an undirected graph G unless $P = NP$.*

Proof. We give the proof for the computation of $c'(G)$. (The proof for $c''(G)$ can be adduced analogously.) Assume that there exists a polynomial time algorithm for the computation of $c'(G)$. Following the proof of Theorem 3 in (Cai, 1983), we show that this implies a polynomial time algorithm for the computation of $\gamma(G)$. (This is sufficient for the proof of the corollary, since it is well known that the computation of $\gamma(G)$ is NP-complete.) Let $G + H$ denote the join of disjoint graphs $G = (V(G), E(G))$ and $H = (V(H), E(H))$, i.e., $G + H = (V', E')$ with $V' = V(G) \cup V(H)$, $E' = E(G) \cup E(H) \cup \{$the edges linking each vertex of G with each vertex of $H\}$. Using the algorithm for determining $c'(G)$ we get a polynomial algorithm for determining the maximum number k $(<n)$ such that $c'(G + K_k) = c'(G)$. (K_k denotes the complete graph with k nodes.)

Since $\gamma(G + K_k) = \gamma(G) + k$, we then conclude from Theorem 2 $\gamma(G) = 2^{c'(G)} - k$. ∎

The $(k > 2)$*-Case*

Due to the last section our adversary knows by now how to make 2-monomials faulty. For arbitrary k-monomials we consider the set of binary $(n \times r)$-matrices (which consists of 2^{nr} elements) and use counting arguments to guarantee the existence of tricky systems of faulty processors without telling the adversary how to construct them. As it will turn out the arguments lead to an upper bound for $f(n, k)$ which is not far away from the trivial lower bound 2^k. The results of the following theorem are closely related to results in (Kleitman and Spencer, 1973).

THEOREM 4. (i) $\forall k, n, (k \leqslant n)$: $f(n, k) \leqslant k \cdot 2^k \cdot \log n \ln 2$.

(ii) *For* $r \geqslant k2^k \log n \ln 2$: *The probability that a randomly chosen binary* $(n \times r)$*-matrix* M_F *is k-faulty approaches* 1, *if n approaches infinity.*

Proof. The results of this theorem are closely related to results in (Kleitman and Spencer, 1973). Here we give a short proof (based on counting arguments), which is sufficient for our purposes.

The number of $(n \times r)$-matrices, which fulfill $A_{i_1}^{\varepsilon_1} \cap \cdots \cap A_{i_k}^{\varepsilon_k} = \varnothing$ for fixed $i_1 = i_2 < \cdots < i_k \leqslant n$ and fixed negation mask $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_k)$, is exactly $(2^k - 1)^r \cdot 2^{(n-k)r}$. Thus, altogether there are at most $\binom{n}{k} \cdot 2^k \cdot (2^k - 1)^r \cdot 2^{(n-k)r}$ non-k-faulty matrices.

To prove (i) it suffices to show, that the fraction of non-k-faulty $(n \times r)$-matrices is strictly less than 1, i.e.,

$$\frac{\binom{n}{k} \cdot 2^k \cdot (2^k - 1)^r \cdot 2^{(n-k)r}}{2^{nr}} < 1$$

for $r \geqslant k2^k \log n \ln 2$. This can be done by some calculations with regard to (1), (2), and (3):

(1) applying the logarithm log to base 2 to the inequality,

(2) using the inequality $y < -\ln(1 - y)$, which can be derived by the Taylor expansion,

(3) observing that $\binom{n}{k} < n^k/2^k$ for $k \geqslant 4$ and doing an extra calculation for $k = 3$.

For part (ii) of the proof it is sufficient to show the existence of a function $\varphi(n)$ with $\varphi(n) \to \infty$ for $n \to \infty$ and

$$2^k \binom{n}{k} (1 - 2^{-k})^r \leqslant 2^{-\varphi(n)}$$

for large n and $r \geqslant k2^k \log n \ln 2$. This inequality can be proven with the same methods as used in the proof of i). ▮

As was mentioned above, Theorem 4 guarantees only the existence of k-faulty systems. We do not know any constructive method to prove the bounds given in the theorem. Nevertheless, a construction of k-faulty systems of size n for the set $[1, r]$ is possible by using one of Friedman's results (1984). (The number r necessary for this construction gives an upper bound for $f(n, k)$ worse than the bounds in Theorem 4.) Instead of $f(n, k)$ ($=\min\{r \mid \exists\ k\text{-faulty system of size } n \text{ in } [1:r]\}$) Friedman considers the function

$$g(n, k) := \min\{r \mid \exists \text{ a collection of } r \text{ partitions of } [1:n] \text{ with property } (*)\}.$$

Property (*) is given by:

> Each partition has exactly k equivalence classes and for any choice of k elements in $[1 : n]$ there exists a partition, such that each equivalence class contains exactly one of the k elements.

According to (Friedman, 1984) $g(n, k) \leqslant \hat{g}(n, k) := \log n \cdot (k^4/\log k) \cdot 2^{2k \log k + 2k}$ and there exists an algorithm which, for given n, k, constructs a suitable collection of $\leqslant \hat{g}(n, k)$ partitions (in time polynomial in n and exponential in k). The following lemma gives a relation between $g(n, k)$ and $f(n, k)$ and thus provides a method to translate results for $g(n, k)$ into results for $f(n, k)$.

LEMMA 4. (i) *A collection of r partitions $P_1, ..., P_r$ with property (*) (for fixed n, k) induces a k-faulty system of size n in $[1:2^k r]$.*

(ii) $f(n, k) \leqslant 2^k \cdot g(n, k)$.

Proof. We have $f(k, k) = 2^k$, since it is necessary and sufficient to make all 2^k monomials in k variables faulty. Thus there exists a k-faulty system of size k in $[1:2^k]$. Let $S = \{S_1, S_2, ..., S_k\}$ be an arbitrary but fixed k-faulty system of size k in $[1:2^k]$.

Assume that the equivalence classes of the r partitions are numbered from 1 to k. This induces a function $\alpha(i, j)$, which associates to an element $i \in [1:n]$ the class number of i with respect to partition P_j. Define for $i = 1, 2, ..., n$:

$$T_i := \bigcup_{j=1}^{r} ((j-1)2^k + S_{\alpha(i,j)}).$$

(As usual, $m + S_l$ denotes the set $\{m + s_l \mid s_l \in S_l\}$.) For different numbers

j_1, j_2 the "translations" $(j_1-1)2^k+S_{\alpha(i,j_1)}$ and $(j_2-1)2^k+S_{\alpha(i,j_2)}$ are subsets of disjoint intervals $[(j_1-1)2^k+1 : j_1 2^k]$ and $[(j_2-1)2^k+1 : j_2 2^k]$ of natural numbers.

To complete the proof observe the following: Let $i_1, i_2, ..., i_k$ be k pairwise different numbers in $[1:n]$. Since the partitions $P_1, ..., P_r$ fulfill property (*), there exists a number j, such that $T_{i_1}, ..., T_{i_k}$ restricted to the jth interval $[(j-1)2^k+1 : j2^k]$ is a translation of the k-faulty system S. Thus $T_1, ..., T_n$ forms a k-faulty system of size n in $[1:r2^k]$ and part (i) of Lemma 4 is proved.

(ii) follows directly form (i). ∎

Using the result from (Friedman, 1984) we immediately get the following:

COROLLARY 3. *A k-faulty system of size n in $[1:\log n \cdot (k^4/\log k) \cdot 2^{2k \log k + 3k}]$ can be obtained constructively.*

Besides the lower bounds 2^k (given in Lemma 2) and $\Omega(\log n)$ (which follows from Theorem 1 and the corollary) we have the following lower bound for $f(n, k)$.

LEMMA 5. *For large n: $f(n, k) \geqslant 2^{k-2} \cdot \log(n-k+2)$.*

Proof. Consider a k-faulty $(n \times r)$-matrix M_F. Then the submatrix M_F^0 (M_F^1) which is obtained by deleting all columns with value 1 (0) in row n and subsequently deleting row n is a $(k-1)$-faulty matrix with $(n-1)$ columns. Thus, we have the recursion $f(n, k) \geqslant 2 \cdot f(n-1, k-1)$. Application of Theorem 1 completes the proof. ∎

We finish this section by comparing upper and lower bounds for some special choices of k:

(1) If k is constant ($\geqslant 2$) the adversary requires $\theta(\log n)$ faulty processors.

(2) If $k = \omega(\log \log n)$ the number of necessary faulty processors is between 2^k and $2^{(1+\varepsilon)\cdot k}$ for almost all n

(3) A gap of k remains in all cases. For instance, for $k = \log \log n$: $f(n, k) = \Omega((\log n)^2)$ and $f(n, k) = O((\log n)^2 \cdot \log \log n)$.

3. The Faulty Link Case

For this section $f^*(n, k)$ denotes the minimum number of faulty links, necessary for an adversary to destroy $k+1$ dimensions (i.e., to make each

$(n-k)$-dimensional subcube faulty). A *faulty link* is uniquely specified by an element $l \in \{0, 1, *\}^n$ which contains exactly one "*" at the position of the non-degenerated dimension. To each set F^* of r faulty links corresponds a $(n \times r)$-matrix $M_{F^*} \in \{0, 1, *\}^{n \times r}$ whose ith column vector gives the ith faulty link. As in the faulty processor case the row vectors may be interpreted as "characteristic vectors" for subsets $A_1, ..., A_n$ of $[1:r] \cup \{(1, *), ..., (r, *)\}$ as follows:

(i) $j \in [1:r]$ is element of $A_i := A_i^1$, iff the ith component of the jth faulty link is "1,"

(ii) $(j, *) \in \{(1, *), ..., (r, *)\}$ is element of A_i^1, iff the ith component of the jth faulty link is "*,"

(iii) $\bar{A}_i := A_i^0$ is a subset of $[1:r]$ and contains j, iff the ith component of the jth faulty link is "0."

The set $A_{F^*} := \{A_1, ..., A_n\}$ is called system of faulty sets. A monomial is called *faulty* with respect to F^*, if the corresponding subcube contains a faulty link from F^*. Formulated in reverse, F^* is called k-faulty, iff it makes each k-monomial faulty.

The above definitions put the situation of faulty links into a framework which is similar to the situation of faulty processors. As in Lemma 1 we have: F^* (resp. M_{F^*}, A_{F^*}) is k-faulty iff for all k-monomials $A_{i_1}^{\varepsilon_1} \cap \cdots \cap A_{i_k}^{\varepsilon_k} \neq \emptyset$. (Observe that the details in the above definitions imply that intersections of sets $A_{i_j}^{\varepsilon_j}$ do not contain elements of $\{(1, *), ..., (r, *)\}$.)

$f^*(n, k)$ can now be interpreted as the minimum r, such that a k-faulty $(n \times r)$-matrix M_{F^*} exists. Of course, $f(n, k) \leqslant f^*(n, k)$, thus all lower bounds of the preceding section remain valid for $f^*(n, k)$. In the following we consider upper bounds for $f^*(n, 2)$ and $f^*(n, k)$ $(k > 2)$.

THEOREM 5. (i) $\forall n$, $f^*(n, 2) \leqslant f(n, 2) + 6$.

(ii) *For large n we even get $f^*(n, 2) \leqslant f(n, 2) + 1$.*

Proof. The proof of (i) follows directly from the recursion

$$f^*(n, k) \leqslant f(n-1, k) + 2 \cdot f^*(n-1, k-1)$$
$$f^*(n, 1) = 3.$$

(Note the following for the correctness of the last equation: It is easy to see that $f^*(n, 1) > 2$. On the other hand, three faulty edges suffice to destroy all $(n-1)$-dimensional subcubes. Take, e.g., $(1, 0, *, ..., 0)$, $(0, *, 1, 1, ..., 1)$, and $(*, 1, 0, 0, ..., 0)$.)

The proof of (ii) is done as follows: we show that, for almost all r, there exists a 2-faulty system A_{F^*} in $[1:r]$, which contains at least

$$s(r) := \binom{r-1}{\lfloor r/2 \rfloor - 1} - \text{polynom}(r)$$

subsets. For large n it then follows directly that $s(r_n + 1) \geqslant n$, which completes the proof!

We now present the construction of the faulty system $A_{F^*} := A$ which is done by forming two subsystems A' and A''.

Construction of A'. Let $r_1 := \lceil r/2 \rceil - 1$, $r_2 := \lfloor r/2 \rfloor - 1$, $I_1 := [1:r_1]$, $I_2 := (r_1 : r-2]$. If r is sufficiently large, then there exist pairwise different sets $P_1, ..., P_{r_1}$ in I_2, each of size $r_2 - 2$, and pairwise different sets $P_{r_1+1}, ..., P_r$ in I_1, each of size $r_1 - 2$.

$A' := \{A_1, ..., A_r\}$ is given by the following definition:

$$\begin{aligned} A_i &:= P_i \cup \{(i, *), r-1, r\} \qquad \forall i = 1, ..., r-2, \\ A_{r-1} &:= P_{r-1} \cup \{(r-1, *), r\}, \\ A_r &:= P_r \cup \{r-1, (r, *)\}. \end{aligned}$$

It is now easy to prove the following properties of A':

(1) Each set in A' contains at most $(r-1)/2$ elements of $[1:r-1] \cup \{(1, *), ..., (r-1, *)\}$ and less than $(r-2)/2$ elements of $[1:r-2] \cup \{(1, *), ..., (r-2, *)\}$.

(2) Any intersection of two sets in A' (except $A_{r-1} \cap A_r$) contains one of the elements $r-1, r$.

(3) Each set A_i with $i \in I_1$ contains all but two elements of I_2 and no element of I_1; and each set A_i with $i \in I_2 \cup \{r-1, r\}$ contains all but two elements of I_1 and no element of I_2.

(4) The systems $\{P_1, ..., P_{r_1}\}$, $\{P_{r_1+1}, ..., P_r\}$ are both antichains.

These properties imply, that A' is a 2-faulty system (for the r-cube).

Construction of A''. We define A'' as the system of all sets $M \subset [1:r]$ of size $\lfloor r/2 \rfloor$ with the following properties:

(a) $r \in M$.

(b) M contains at least three elements of I_j $(j = 1, 2)$.

(c) At least three elements of I_j $(j = 1, 2)$ are missing in M.

It is now easy to prove the following properties of A'':

(1) Each set in A'' contains less than half of the elements of $[1:r-1]$.

(2) Any intersection of two sets in A'' contains r.

(3) A'' is an antichain.

These properties imply that A'' is a 2-faulty system.

The following claims complete the proof of Theorem 5.

Claim 1. $A := A' \cup A''$ is a 2-faulty system.

For the proof of Claim 1 it remains to show that the sets $M' \cap M''$, $\bar{M}' \cap \bar{M}''$, $M' \cap \bar{M}''$, $\bar{M}' \cap M''$ with $M' \in A'$, $M'' \in A''$ are never empty. This follows from property (1) of A' and A'' for $\bar{M}' \cap \bar{M}''$, property (3) of A' and (b) of A'' for $M' \cap M''$, property (3) of A' and (c) of A'' for $M' \cap \bar{M}''$, property 3 of A' and (b) of A'' for $\bar{M}' \cap M''$.

Claim 2. $|A| \geqslant |A''| \geqslant \binom{r-1}{\lfloor r/2 \rfloor - 1} - O(r^6)$.

A straightforward computation shows that the number of sets M which are excluded by properties (a), (b), (c), can be bounded by a polynomial of degree 6. ∎

Note that the recursion given at the beginning of the above proof relates $f^*(n, k)$ to $f(n, k)$ and thus gives the possibility to construct k-faulty matrices M_{F^*} with the help of Corollary 3. This leads to (constructive) upper bounds for $f^*(n, k)$. Analogously to Theorem 4 we obtain better (but nonconstructive) upper bounds in the following:

THEOREM 6. (i) $\forall k, n, (k \leqslant n)$:

$$f^*(n, k) \leqslant k \cdot 2^k \cdot \frac{n}{n-k} \cdot \log n \ln 2.$$

(ii) *For* $r \geqslant k 2^k (n/(n-k) \log n \ln 2$:

The probability that a randomly chosen $(n \times r)$*-matrix* M_{F^*} *is* k*-faulty approaches* 1, *if* n *approaches infinity.*

Proof. We omit the proof. It can be produced analogously to the proof of Theorem 4. ∎

4. A FAULT-CHECKING PROCEDURE

We describe a simple, distributed fault-checking procedure on the n-cube, which is considered as a synchronous network. The restriction to a synchronous network is not essential but simplifies the description of the algorithm.

The following notations are used for all $\alpha \in \{0, 1\}^n$, $s \in [0:n]$:

α^i denotes the vector which only differs from α in the ith bit.

$C_\alpha(s) := X_1^{\alpha_1} \cdots X_s^{\alpha_s}$ is the (unique) $(n-s)$-dimensional subcube which contains α and is degenerated with respect to the first s dimensions. ($C_\alpha(0)$ denotes the whole cube.)

$\mathrm{Dim}_\alpha := \max\{n-s \mid C_\alpha(s) \text{ is nonfaulty}\}$

THEOREM 7. *There exists a distributed algorithm which computes* Dim_α *in* $O(n)$ *parallel steps for all* α.

Proof. We assume that each processor α has a register D_α which, at the beginning, is initialized by n and, at the end of the computation, should have value Dim_α. In a constant number of steps each processor α can execute a procedure $\mathrm{faulty}_\alpha(i)$. This procedure returns "true," if α^i or the link between α and α^i is faulty, otherwise it returns "false." The algorithm is then given by the following fragment of pseudo Pascal:

```
for i := 1 step 1 to n do
     begin
     forall α ∈ {0, 1}^n
     pardo begin
             if faulty_α(i)
                  then D_α := min{D_α, D_α^i}
             end;
  end;
```

For each $\alpha \in \{0, 1\}^n$ and each $s \in [0:n]$ we call subcube $C_\alpha(s)$ *secure*, iff

(i) $\forall$ nonfaulty $\beta \in C_\alpha(s)$: $D_\beta \geqslant n-s$

(ii) if $C_\alpha(s)$ is nonfaulty, then $\min\{D_\beta \mid \beta \in C_\alpha(s)\} = \mathrm{Dim}_\alpha$.

Since all registers D_α are initialized by n, at the beginning all subcubes $C_\alpha(0)$ (i.e., the whole n-cube) are secure. Now it is not difficult to show that, if all subcubes $C_\alpha(s)$ are secure before a run through the **for**-loop, then all subcubes $C_\alpha(s+1)$ are secure after the run. Thus, after n runs through the loop all subcubes $C_\alpha(n)$, i.e., all processors are secure. But, as follows from the definition of "secure," for a nonfaulty processor α which is secure we get: $D_\alpha = \mathrm{Dim}_\alpha$. This completes the proof. ∎

The abovementioned distributed algorithm checks only subcules of the form $X_1^{\alpha_1} \cdots X_s^{\alpha_s}$ for correctness. Thus, it does not always find the maximum dimension of a surrounding faultless subcube. Nevertheless, $\mathrm{Dim}_\alpha \geqslant n - \lfloor \log r \rfloor - 1$ for some α if the number of faults is r. Note that this, for example, is nearly optimal in the following case: r faults destroy k dimensions with $k = \omega(\log\log n)$ and $r = f(n, k)$. As mentioned above, this implies $2^k \leqslant r = f(n, k) \leqslant 2^{(1+\varepsilon)k}$!

5. Concluding Remarks

The Notion of the Directed Chromatic Index

The notion of the directed chromatic index is interesting in its own right. This can be illustrated by the following brief considerations:

(a) The notion of directed chromatic indices c' and c'' of undirected graphs leads to classes of $C'(s)$ and $C''(s)$ of graphs whose edges can be coloured with no more than s colours. For instance, $C'(1) = C''(2)$ is the class of bipartite graphs, $C'(2)$ contains the class of planar graphs iff the 4-colour conjecture is true. As a corollary, since the 4-color conjecture has been proven (Appel *et al.*, 1977), the set of edges of each planar graph $G = (V, E)$ splits into 2 sets E_1 and E_2 such that the corresponding partial subgraphs $G_i = (V, E_i)$ are bipartite; i.e., they do not contain an odd cycle. Results corresponding to other choices of s are omitted in the framework this paper.

(b) The inherently intractable problem of computing the chromatic number of a given graph can be broken up into 2 parts according to the following question: Is it possible to compute the chromatic number of G assuming that an oracle reports simplest, directed versions of G?

Unsolved Problems

The following questions are left unanswered by this paper:

Can $f(n, k)$ be determined more precisely?

How can the adversary who accomodates to given fault-checking procedures be analysed when $k \geqslant 3$?

What are efficient designs of fault-checking procedures (the associated graph for $k = 2$ should have a big chromatic number)?

Consider "embeddings" of m-cubes $(m < n)$ in the functioning part of an n-cube with faults. Allow embeddings which map adjacent nodes not necessarily to adjacent nodes but to nodes at small distance apart. How can these embeddings be constructed? What is the maximum dimension m of an embedded cube for a given fault distribution? Answers to these questions are given in (Hastad *et al.*, 1987) for the case that nodes are faulty with fixed probability p and faults are randomly distributed.

ACKNOWLEDGMENTS

The authors thank Nick Pippenger, who pointed out the relevance of Joel Friedman's paper for their purposes; also many thanks to Ludek Kucera who discovered the recurrence relation given in the proof of Lemma 5.

RECEIVED May 21, 1987; ACCEPTED September 1987

REFERENCES

APPEL, K., HAKEN, W., AND KOCH, J. (1977), Every planar map is 4-colourable, *Illinois J. Math.* **21**, 429–567.

CHUNG, F. R. K., AND GAREY, M. R. (1983), Diameter bounds for altered graphs, unpublished manuscript.

CAI, M. C. (1983), Solutions to Edmond's and Katona's problems on families of separating subsets, *Discrete Math.* **47**, 13–21.

DILWORTH, R. P. (1950), A decomposition theorem for partially ordered sets, *Ann. of Math. (2)* **51**, 161–166.

FRIEDMAN, J. (1984), Constructing $O(n \log n)$ size monotone formulae for the kth elementary symmetric polynomial of n Boolean variables, *in* "Proceedings, 25th IEEE Found. of Comput. Sci., pp. 506–515.

HASTAD, J., LEIGHTON, T., AND NEWMAN, M. (1987), Reconfiguring a hypercube in the presence of faults, *in* "Proceedings, 19th ACM Sympos. Theory of Comput," pp. 274–284.

KLEITMAN, D. J., AND SPENCER, J. (1973), Families of k-independent sets, *Discrete Math.* **6**, 255–262.

PEASE, M. C. (1977), The indirect binary n-cube microprocessor array, *IEEE Trans. Comput.* **C-26**, No. 5, 458–473.

PREPARATA, F. P., AND VUILLEMIN, J. (1981), The cube-connected cycles: A versatile network for parallel computation, *Commun. ACM* **24**, No. 5, 300–309.

SCHÖNHEIM, J. (1971), A generalization of results of P. Erdös, G. Katona, and D. J. Kleitman concerning Sperner's theorem, *J. Combin. Theory Ser. A* **11**, 111–117.

SIEGEL, H. J. (1979), A model of SIMD mashines and a comparison of various interconnection networks, *IEEE Trans. Comput.* **C-28**, No. 12, 907–917.

SPERNER, E. (1928), Ein Satz über Untermengen einer endlichen Menge, *Math. Z.* **27**, 544–548.

Printed in Belgium